Digital Image Forgery Detection by Local Statistical Models

Jiří Grim, Petr Somol
Institute of Information Theory and Automation
Academy of Sciences of the Czech Republic
Pod vodarenskou vezi 4
CZ-182 08 Prague 8, Czech Republic
E-mail: (grim,somol)@utia.cas.cz

Pavel Pudil
Faculty of Management
Prague University of Economics
Jarošovská 1117/II
CZ-377 01 Jindřichův Hradec, Czech Republic
E-mail: pudil@utia.cas.cz

***Abstract*—We propose an application of local statistical models in the form of a locally estimated Gaussian mixture to image forgery detection. The estimated mixture is used to compute the so called log-likelihood transformation of the original image. We show that image manipulations of different type may be visible in a suitably designed log-likelihood image. Unlike other methods the forgery detection based on local statistical model is rather non-specific and suitable to emphasize various traces of possible image tampering without any prior information.**

***Keywords*-forgery detection; local statistical models; distribution mixtures; EM algorithm;**

I. Introduction

The advanced digital imaging technologies and widely available image editing software make it very easy to manipulate digital images. As a consequence there is an increasing need to verify the authenticity of images or image sources in many areas and for various purposes. One of the most common and difficult problems is to expose the traces of possible tampering in a given image of unknown origin without any previous information. In the last years several approaches have been proposed with the aim to detect image forgery of different types (cf. [5]). Usually they are based on different highly specific image processing aspects.

One of the most typical ways to manipulate an image is to insert and splice image parts of different origin. This type of image manipulation typically involves several image processing operations such as scaling, rotation, brightness modification, smoothing, adding noise etc. For this purpose there are many editing procedures available. Usually, these procedures require resampling of the source image parts onto a new sampling lattice by using interpolation. This interpolation, though often imperceptible, introduces specific correlations into the image which can be used to detect the underlying digital tampering. Popescu and Farid [10] proposed an interesting technique based on EM algorithm to identify the periodicities arising in the manipulated images. Mahdian and Saic [9] succeeded to describe analytically the specific periodic properties of the interpolated images and proposed detection of resampling by using derivative operator and Radon transformation. The resampling detection method is able to identify broad range of resampling rates in uncompressed TIFF and JPEG images and is reasonably resistant to simple counter-measures. However, the detection performance decreases with the lossy JPEG format. Also, by adding noise, the interpolation based periodicity becomes difficult to detect.

In a recent paper Popescu and Farid [11] proposed a similar way to identify the effects of resampling on color-filter-array interpolated images. They make use of the fact that most digital cameras contain only one sensor array combined with a color filter mask. Thus only a single color sample is recorded at each pixel location and the other two color samples must be interpolated from the neighboring pixels. Again, this interpolation introduces specific identifiable periodicities. The presence or lack of interpolation based periodicities can be used to expose possible image manipulation. Expectedly, the detection accuracy decreases with the decreasing JPEG compression quality. A successful but difficult "counter-measure" would be to re-sample and re-interpolate the tampered image.

Johnson and Farid [7] proposed a method based on inspecting lighting conditions. Approximating the lighting environment by a simple model they are able to identify inconsistencies which can be used to detect possible image manipulation. The approach is less efficient when the lighting conditions of the original and forged objects are similar or when no directional light source was present.

One of the early methods (cf. Fridrich et.al [6]) tries to identify the copy-move forgery, when a part of an image is duplicated elsewhere in the same image. Simple matching between square pixel blocks is rather successful to identify exact replicas but the algorithm might fail in flat uniform areas. In a more robust version the matching uses representation of blocks in JPEG format.

Since the majority of digital cameras store images in JPEG format, it is likely that both the original and forged images are stored in this format. The resulting double JPEG compression introduces identifiable periodic pattern into the histograms of the underlying DCT coefficients (cf. Lukas and Fridrich [8]). However, a double JPEG compression may naturally arise e.g. by re-saving a high quality image with a

lower quality and therefore it is of limited relevance only.

In this brief overview we do not discuss several other forensic approaches related to authentication of images (e.g., watermarking) or assuming specific knowledge of unique camera-specific properties (e.g., camera response function, camera pattern noise, sensor imperfection map, color filter array defects etc.), or related to other problems (camera identification).

In the following we propose application of local statistical models to image forgery detection. The method has been recently applied to evaluation of screening mammograms [4]. It appears that, unlike other approaches, the statistical model in the form of a multivariate distribution mixture is suitable to emphasize rather non-specific traces of possible tampering.

II. Local Statistical Model

Originally we have proposed the local statistical models in connection with texture modeling [2]. Typical texture images are highly stochastic but relatively homogeneous and therefore it is reasonable to assume that the local statistical texture properties do not change very much. We have suggested to estimate the joint probability distribution of pixel values (grey levels or color channels) within a suitably chosen sliding window. The estimated model in the form of a distribution mixture of product components can be used to synthesize arbitrarily large texture images by prediction. Simultaneously we have a unique possibility to verify the model quality by comparing the synthesized texture with the original sample. Motivated by good results of texture modeling [2] we have applied the mixture model to the local evaluation of the original "source" texture image [3]. Thus the local statistical model has been used to evaluate textures (cf. Grim et al. [3]) and in the screening mammography as a decision-supporting tool (cf. Grim et al. [4]). In this paper we show that various traces of image tampering can also be emphasized by using the local model in a similar way.

From the computational point of view the method is based on estimating local statistical properties of the image in terms of joint probability distribution of pixel color samples within the reference window. The probability distribution in the form of a Gaussian mixture is estimated by EM algorithm from the data set $\mathcal{S}$ obtained by sliding the window throughout the image. In particular, given an observation window centered at a position (i, j) we denote

$$\boldsymbol{x}(i,j) = \boldsymbol{x} = (x_1, x_2, \ldots, x_N) \in \mathcal{X}, \quad \mathcal{X} = R^N$$

the vector of spectral values of the window pixels in a fixed arrangement; thus for each pixel there are three spectral values in the vector $\boldsymbol{x}$. In each position we treat the window contents (the window patch) $\boldsymbol{x} \in \mathcal{S}$ as an observation of a random vector and approximate the unknown density function $P(\boldsymbol{x})$ in the form of Gaussian mixture of product components

$$P(\boldsymbol{x}) = \sum_{m \in \mathcal{M}} w_m F(\boldsymbol{x}|\boldsymbol{\mu}_m, \boldsymbol{\sigma}_m), \quad \boldsymbol{x} \in \mathcal{X}. \tag{1}$$

Here $\mathcal{M} = \{1, \ldots, M\}$ and $\mathcal{N} = \{1, \ldots, N\}$ denote the index sets of components and variables respectively, w_m are the component weights and $F(\boldsymbol{x}|\boldsymbol{\mu}_m, \boldsymbol{\sigma}_m)$ denote the product components [2], [3]:

$$F(\boldsymbol{x}|\boldsymbol{\mu}_m, \boldsymbol{\sigma}_m) = \prod_{n \in \mathcal{N}} f_n(x_n|\mu_{mn}, \sigma_{mn}), \tag{2}$$

$$f_n(x_n|\mu_{mn}, \sigma_{mn}) = \frac{1}{\sqrt{2\pi}\sigma_{mn}} \exp\left\{-\frac{(x_n - \mu_{mn})^2}{2\sigma_{mn}^2}\right\}$$

The corresponding log-likelihood function

$$L = \frac{1}{|\mathcal{S}|} \sum_{x \in \mathcal{S}} \log\left[\sum_{m \in \mathcal{M}} w_m F(\boldsymbol{x}|\boldsymbol{\mu}_m, \boldsymbol{\sigma}_m)\right] \tag{3}$$

can be maximized by means of the following EM iteration equations (cf. [1], [3]): $(m \in \mathcal{M}, n \in \mathcal{N}, \boldsymbol{x} \in \mathcal{S})$

$$q(m|\boldsymbol{x}) = \frac{w_m F(\boldsymbol{x}|\boldsymbol{\mu}_m, \boldsymbol{\sigma}_m)}{\sum_{j \in \mathcal{M}} w_j F(\boldsymbol{x}|\boldsymbol{\mu}_j, \boldsymbol{\sigma}_j)}, \tag{4}$$

$$w_m^{'} = \frac{1}{|\mathcal{S}|} \sum_{x \in \mathcal{S}} q(m|\boldsymbol{x}), \tag{5}$$

$$\mu_{mn}^{'} = \frac{1}{w_m^{'}|\mathcal{S}|} \sum_{x \in \mathcal{S}} x_n q(m|\boldsymbol{x}), \tag{6}$$

$$(\sigma_{mn}^{'})^2 = \frac{1}{w_m^{'}|\mathcal{S}|} \sum_{x \in \mathcal{S}} (x_n - \mu_{mn}^{'})^2 q(m|\boldsymbol{x}). \tag{7}$$

Here the apostrophe denotes the new parameter values in each iteration.

The estimated mixture can be used to compute the probability density values $P(\boldsymbol{x})$ at each position of the window. The basic idea of our method is to display the suitably scaled log-likelihood value $\log P(\boldsymbol{x})$ as a grey level at the central pixel of the window. In this way we actually transform the original color image to a grey-scale image showing the local log-likelihood values of the mixture model. In the resulting log-likelihood image the light pixels correspond to the typical window locations and dark pixels to the less typical ones.

In case of image forgery detection any "unnatural" local changes of the log-likelihood image may be relevant. In this sense, if μ_0 and σ_0 are the mean and variance of the log-likelihood values $\log P(\boldsymbol{x})$ respectively, then a reasonable choice of the displayed interval is

$$\log P(\boldsymbol{x}) \in \langle \mu_0 - 2 * \sigma_0;\ \mu_0 + 2 * \sigma_0 \rangle.$$

Obviously the form and size of the reference window is of importance, too. In case of image analysis the window should be nearly circular to reflect the neighborhood of the central pixel optimally. Since a large window tends to

smooth out small details and slows down the computation we have considered relatively small square window of 5x5 pixels with trimmed corners. The resulting 21 window pixels imply in three color channels the model dimension N=63. In other words, each value $P(\boldsymbol{x})$ of the estimated mixture density is determined by 63 color sample values x_n of the window patch. It is intuitively clear that even small changes of the image details may strongly influence the corresponding log-likelihood values $\log P(\boldsymbol{x})$. In this sense the log-likelihood image can be useful to emphasize various traces of image manipulation.

III. Experimental Results

In general, the present image forgery detection methods do not allow strict conclusions. They are usually designed to reveal only specific types of tampering, they have weak points, their accuracy decreases with lossy compression formats and the results of detection are not always convincing. Probably, even in the future, it will be necessary to try to identify suspect locations by all available methods.

Since there is no generally accepted benchmark for image forgery detection, we illustrate the properties of our method by examples - as usual in literature. In particular, an inserted and possibly modified image part of unknown origin would be identified because of potential differences between the source and target image. Even slightly different features like brightness, resolution, textural properties, lighting conditions, traces of resampling or others may cause visible changes in the log-likelihood image (cf. Fig. 1).

Another more specific detection mechanism relates to image frequency content. Formally, the component means $\boldsymbol{\mu}_m$ correspond to weighted averages of the sample vectors $\boldsymbol{x} \in \mathcal{S}$ (cf. (6)) and therefore they are rather smooth without high frequency details. If the frequency content of the inserted image portion is modified (e.g. by resizing, subsampling, or interpolation) then the corresponding region may become visible in the log-likelihood image. Thus, an inserted slightly blurred region (cf. Fig. 2, left) appears lighter because of better fitting of component means. For analogous reasons the increased high frequency content (e.g. by sub-sampling) would darken the corresponding part of the log-likelihood image. Fig. 3 shows a picture assembled from three different parts by autostich software. The medium slightly blurred (incorrectly focused) part becomes lighter in the log-likelihood image (right) because of the missing high frequencies. Some autostich artifacts in the blue sky region are also visible.

In comparison with other techniques [6], [7], [8], [10], the image forgery detection by local statistical models could be more resistent to lossy information compression since, as long as there is no essential image degradation, the differences between the local image properties should be detectable. For example, in Fig. 2 the evaluated image is JPEG compressed with the quality 70%.

There is an interesting possibility to apply the proposed method to a suitably transformed image. In this way we could identify for example the periodicities arising in the interpolated images. If we compute the local statistical model from the spectral deviations of the original image and its smoothed version then the corresponding log-likelihood image would show the underlying periodicities.

IV. Concluding Remarks

The proposed image forgery detection by local statistical models is a blind method applicable to the images of unknown origin without any prior information. Generally, the underlying log-likelihood image is capable to emphasize local changes of the image properties. For this reason the method could be useful to expose suspect regions of possible tampering of various kinds. The results are reasonably resistent to lossy information compression.

Acknowledgment

This work was supported by the projects GAČR No. 102/07/1594 and 102/08/0593 of the Czech Grant Agency and partially by the MŠMT projects 2C06019 ZIMOLEZ and 1M0572 DAR.

References

[1] A.P. Dempster, N.M. Laird and D.B. Rubin. Maximum likelihood from incomplete data via the EM algorithm. *Journal of the Royal Statistical Society*, **B 39**, 1–38, 1977.

[2] J. Grim, M. Haindl, P. Somol, and P. Pudil. A subspace approach to texture modelling by using Gaussian mixtures. In *Proc. of the 18th Int. Conf. ICPR 2006*, Eds. B. Haralick, T.K. Ho), pp. 235–238, 2006.

[3] J. Grim, P. Somol, M. Haindl, and P. Pudil, A statistical approach to local evaluation of a single texture image. In *Proc. of the 16-th Symp. PRASA 2005*. Ed. F. Nicolls, pp. 171–176, 2005. (for full text version cf. *http://www.prasa.uct.ac.za/*)

[4] J. Grim, P. Somol, M. Haindl, J. Danes. Computer-Aided Evaluation of Screening Mammograms Based on Local Texture Models, *IEEE Transactions on Image Processing*, Vol. 18, No. 4 (2009), pp. 765-773.

[5] Farid, H. Image forgery detection, *IEEE Signal Processing Magazine*, Vol.26, No.2 (2009) pp. 16-25

[6] J. Fridrich, D. Soukal, and J. Lukas. Detection of copy-move forgery in digital images. In *Proceedings of DFRWS*, 2003.

[7] M.K. Johnson and H. Farid. Exposing digital forgeries by detecting inconsistencies in lighting. In *ACM Multimedia and Security Workshop*, New York, NY, 2005.

[8] J. Lukas and J. Fridrich. Estimation of primary quantization matrix in double compressed JPEG images. In *Digital Forensic Research Workshop*, Ohio, 2003.

[9] B. Mahdian and S. Saic. Blind Authentication Using Periodic Properties of Interpolation. *IEEE Transactions on Information Forensics and Security*, 3(3):529538, 2008.

[10] A.C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing*, 53(2):758767, 2005.

[11] A.C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, 53(10):39483959, 2005.

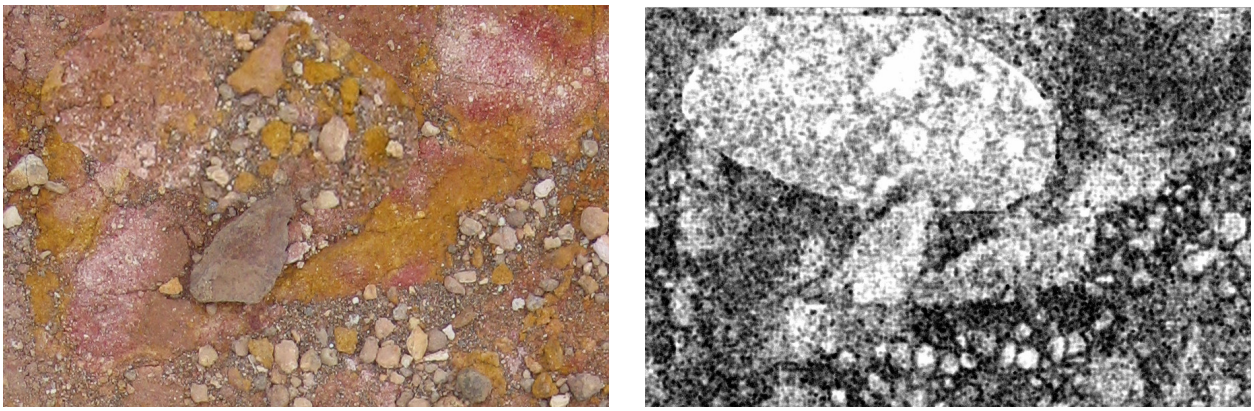

Figure 1. The oval part in the left-upper corner having somewhat different textural properties becomes distinctly lighter in the log-likelihood image.

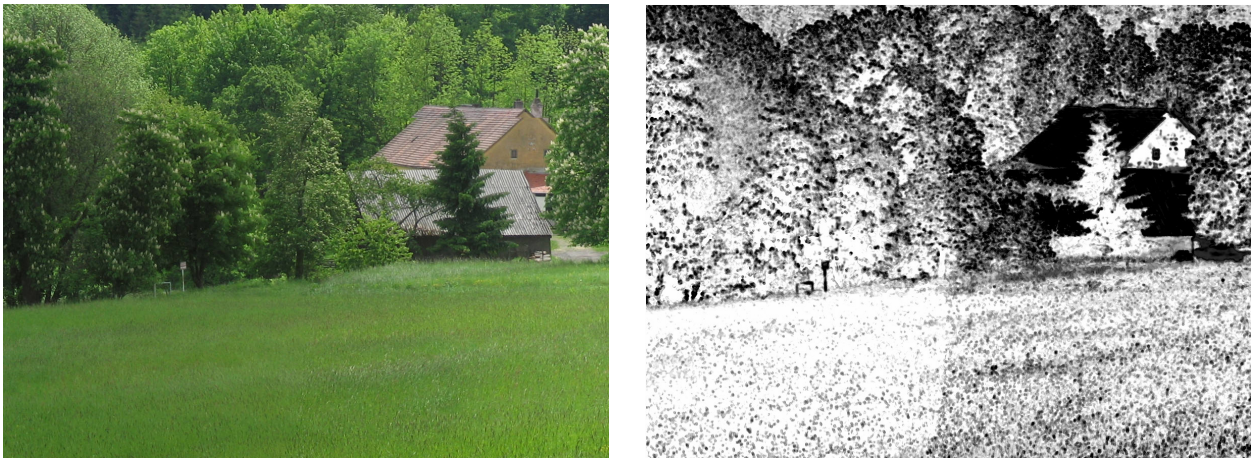

Figure 2. Example of an image assembled from two parts by autostitch software. The slightly blurred left part becomes lighter in the log-likelihood image (right) because of missing high-frequency details. The analyzed image is JPEG compressed with the quality 70%.

Figure 3. Picture assembled from three parts by autostitch software. The medium slightly blurred (incorrectly focused) part becomes lighter in the log-likelihood image (right). In the blue sky region there are also visible artifacts caused by panoramic stitching.